

Results 1 - 10 of about 184,000 for pedersen commitment scheme. (0.16 seconds)

Web



Show options...

1. [PS] 1 Commitment Schemes

File Format: Adobe PostScript - View as HTML

2.5 Pedersen commitment (using discrete log). Finally, we give an example of a commitment scheme based on a specific number theoretic ...

cs.nyu.edu/courses/fall01/G22.3033-003/lect/lecture14.ps - Similar

2. [PS] An Integer Commitment Scheme based on Groups with Hidden Order

File Format: Adobe PostScript - View as HTML

scheme of Pedersen [6], for the associated protocols and additional ... an integer commitment scheme, as well as a zero-knowledge protocol for prov- ...

www.daimi.au.dk/~ivan/papers/gencommit.ps - Similar

by I Damgaard - 2001 - Cited by 146 - Related articles - All 17 versions

3. **PPT** CS 380S - Theory and Practice of Secure Systems

File Format: Microsoft Powerpoint - View as HTML

Pedersen Commitment Scheme. Setup: receiver chooses... Large primes p and q such that q divides $p-1$; Generator g of the order- q subgroup of \mathbb{Z}_p^* ...

www.cs.utexas.edu/~shmat/courses/cs380s fall08/17zk.ppt - Similar

4. [PDF] Lecture Mutually Independent Commitments 1 Introduction ...

File Format: PDF/Adobe Acrobat - View

Although A's commitment to p does not reveal anything, a commitment scheme like

Pederson's would allow B to commit to $p+1$ just by seeing $C(p)$

ocw.mit.edu/NR/rdonlyres/Electrical...and.../lec041603.pdf - Similar

5. **[PPT]** Verifiable Threshold Secret Sharing and Full Fair Secure Two-party ...

File Format: Microsoft Powerpoint - View as HTML

Pedersen gave a semantically secure **commitment scheme** based on the difficulty of discrete logarithm problem, and proposed a **VTSS scheme** in the CRS model by ...

sersc.org/...Verifiable%20Threshold%20Secret%20Sharing%20and%20Full%20...

- Similar

6. "COMMITMENT SCHEME" related terms, short phrases and links

(Web site); We develop provably secure and efficient OCBE protocols for the Pedersen commitment scheme and comparison predicates as well as logical ...
keywen.com/en/COMMITMENT SCHEME - Cached - Similar

7. CiteSeerX — Practical and Provably-Secure Commitment Schemes from ...

50, On the existence of statistically hiding bit commitment schemes and fail-stop signatures – Damgard, Pedersen, et al. - 1997 ...
citeseer.ist.psu.edu/halevi96practical.html - [Cached](#) - [Similar](#)
by S Halevi - 1996 - Cited by 80 - Related articles - All 9 versions

8. [PDF] MTAT.07.003 Cryptology II Commitment Schemes

File Format: PDF/Adobe Acrobat - View

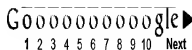
Pedersen commitment scheme. Setup: Let q be a prime and let $G = \langle g \rangle$ be a q -element DL-group. Choose y uniformly from $G \setminus \{1\}$ and set $pk \leftarrow (q, y)$
www.cs.ut.ee/~swen/courses/crypto-ii/06-commitments.pdf - Similar

9. A Straight-Line Extractable Non-malleable Commitment Scheme

As in the case of Pedersen's commitment scheme [11], we see the scheme is computationally binding under the DLA. 4. Equivocality and Extractability of the ...
ietfex.oxfordjournals.org/cgi/reprint/E90-A7/1384.pdf - Similar
 by S Arifa - 2007 - Cited by 1 - Related articles

10. Efficient Non-malleable Commitment Schemes

But if we too use **Pedersen's commitment scheme** with the public generators $g, 0$, h , 0 to commit to value a in this coin-flipping proto- ...
www.springerlink.com/index/NEUARWBCBA4EW7YE.pdf - Similar
 by M Fischlin - Cited by 52 - Related articles - All 19 versions



pedersen commitment scheme

Search

[Search within results](#) - [Language Tools](#) - [Search Help](#) - [Dissatisfied? Help us improve](#) - [Try Google Experiments](#)

